Secure Data Aggregation Technique in Wireless Sensor Network: A Survey

Punam Dandare
Department of Computer Science and Engineering
G. H. Raisoni Academy of Engineering and Technology, Nagpur, India

Vikrant Chole
Department of Computer Science and Engineering
G. H. Raisoni Academy of Engineering and Technology, Nagpur, India

Shruti Kolte
Department of Computer Science and Engineering
G. H. Raisoni Academy of Engineering and Technology, Nagpur, India

ABSTRACT

Wireless sensor networks (WSNs) consist of sensor nodes. It is a collection of wild number of low cost device constraint sensor nodes that communicates using wireless medium and they are small in size, low battery power and limited processing capability. This restraint of low electricity power of a sensor node and limited energy capability makes the wireless sensor network failure. A data aggregation is very important techniques in wireless sensor networks and it reduces the energy consumption by eliminating redundancy. In WSNs, Sensor nodes are resources constrained in memory, data sensing, and battery power and communication capability. Data communication is the process of communications between nodes that consumes a large portion of the total amount of energy used up for WSNs. One of the solutions to reduce number of bits transmitted during communication is data aggregation. As wireless sensor networks are usually deployed in remote and hostile environments to trajectory sensitive information or data, sensor nodes are affected by attacks. Thus, security is an important issue to be considered in WSNs.

General Terms

Data Security, Secure data Aggregation, Iterative Filtering Algorithm, Secure data aggrgation algorithms et. al.

Keywords

Data Aggregation, Wireless sensor network, security

1. INTRODUCTION

Wireless Sensor Network is a network of several hundreds or even thousands, where each node is connected to one sensor. WSN are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network. WSN are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The network is small sized, low cost sensor nodes, which senses the remote and hostile environment and communicate the network for information gathered from the data analysis field through wireless links.

Data aggregation is the process of data gathering, aggregating and collecting the useful data for wireless network. In WSNs, data aggregation is the process to save the energy, resources and a network lifetime. The main cause of data aggregation algorithms is to tally the data and aggregate that data in an energy efficient privacy manner, so that the period of network lifetime is enhanced and the power is optimized. In this paper, different data aggregation technique, various privacy preserving energy-efficient algorithm and security process for data aggregation on wireless sensor networks are presented.

1.1 Data Aggregation

The data aggregation is a technique in WSNs used to solve the implosion and overlap problems in data centric routing protocols. Data coming from multiple sensor nodes are aggregated as if they are about the same attribute of the phenomenon when they reach the same routing node on the way back to the sink. Data are aggregated from various sensor nodes by using data aggregation technique. The security issues, i.e., data confidentiality and data integrity, data aggregation become necessary when the sensor network is organized in a hostile and remote environment.

Data aggregation is the process of collecting the sensor data in network using aggregation and it uses the dynamic routing protocol for aggregation, then the data aggregation algorithm uses the sensor data from the sensor nodes and then combine the sensor data by using some data aggregation algorithms, i.e. LEACH (Low Energy Adaptive Clustering Hierarchy), SPIN (sensor protocol for data via negotiation), PEGASIS (Power- Efficient Data-Gathering Protocol for Sensor Information Systems), TAG(Tiny Aggregation), AODV(Ad hoc On Demand Distance Vector) etc.

2. LITERATURE REVIEW

2.1 SIA: Secure Information Aggregation

S. Ganeriwal, L. K. Balzanet. al. [1], the work is related to the trust and reputation systems in WSNs. It was proposed a general reputation framework for sensor networks in which each node develops reputation estimation for sensors nodes by observing its neighbors which make a trust system community for sensor nodes in the network. They proposed Secure Information Aggregation (SIA) [7], which has the information obtained from neighboring nodes, is a kind of secondhand information and the authenticity of its sources and the integrity of their contents cannot be guarantees directly. However, these systems do not fit all the requirement and features required by WSN. Trust and reputation systems have a significant role in supporting operation of distributed systems, from wireless sensor networks and e-commerce infrastructure to social networks, thus reputation based trust systems are employed to detect abnormal activities and enhance the trustworthiness among sensors by providing an assessment of trustworthiness of participants in such distributed systems.

2.2 SDA: Secure Data Aggregation

SuatOzdemir, Yang Xiaoet. al. [2], presents Secure Data Aggregation (SDA), it is the process to mitigate the equal data transmission in the wireless network. Data Aggregation is way of summarizing and combining sensor data. Data aggregation is the process of data summarizing that has the security challenges in secure data aggregation. In SDA [8], Data aggregations are confidentially and integrity of data that are used for encryption data. As wireless sensor networks are deployed in remote system and hostile environments to send sensitive message, sensor nodes are inclined to settlement of a dispute by giving up something on both sides of attacks and the security issues in data confidentiality and integrity are very important in WSNs. Hence, wireless sensor system protocols for data aggregation, e.g. Data aggregation protocol, must be planned with security and investigates the relationship between security and aggregation process in WSNs. The aggregators in secure data aggregation need to decrypt the encrypted data to perform aggregation.

2.3 SRDA: Secure Reference-Based Data Aggregation

X.-Y. Xiao, W.-C.Peng, C.-C. Hung et. al. [3], proposed Secure Reference-Based Data Aggregation (SRDA), a trust based framework in WSNs which employs correlation to detect faulty readings by using an Iterative Filtering algorithm. They propose an innovative in-network voting scheme that consist of hundreds of thousands tiny sensors node that works together to do some task for determining faulty readings by taking the reliable node between the correlation of reading in a WSNs. Detecting node with defective readings is the one challenging issues in WSNs to obtain the sensor readings by evaluating the construction of a logical correlation network. The correlation function of the chain in the network , it can be describe by a set of vertices and edges of a network, these mechanisms for correlation rating sensors is called sensor rank [9], where each vertex describes a sensor node and a wedge between two sensor nodes denotes their correlation readings. If two nearby nodes have their same edges, then these nodes have false readings. Therefore, only sensor nodes have correct readings which are connected by correlation edges of the network. The weighted voting method uses the correlation between sensor nodes as weights. Moreover, they introduced a ranking framework to associate a level of trustworthiness with each sensor node based on the number of neighboring sensor nodes are supporting the sensor and trustworthiness of the secure data aggregation in WSNs.

2.4 MAX-MIN AND CPDA: Cluster-based Private Data Aggregation AND SMART: Slice-Mix-AggRegaTe

He, W., Liu, X., Nguyen, H. V., Nahrstedt, K et. al. [4], present on privacy -preserving data aggregation scheme for energy efficiency, which can be extensive to approximate MAX-MIN aggregation function. The First method MAX-MIN aggregation is one of the aggregation functions that work to extract the readings of the entire sensor network in the maximum and minimum readings. They proposed an effective mechanism for a MAX-MIN aggregation in WSN that is called Sensor MAX-MIN Aggregation (SMMA). It aggregates data in an energy efficient manner and get accurate aggregate result. The second method Cluster-based Private Data Aggregation (CPDA) is a clustering protocol. CPDA method in which a data is aggregated from cluster members and create a cluster head for the network. For this, clusters head perform data aggregations. It has the great advantage of incur less communication overhead and nodes have public and private data. To perform aggregation, sensor nodes have high communication cost because a large numbers of communication is needed. The third scheme Slice-Mix-AggRegaTe (SMART) method to carry out private data preservation by using a slicing technique in data aggregation. For this, each sensor node select a set of nodes by chance within n hops and slices its own private data into m pieces randomly for this aggregation private data preservation builds a slicing data techniques. When a sensor node receives the sliced data from a nearer node, it collects received data and sends the outcome to the sink node in WSNs. SMART method also endure from high communication cost because each sensor node should share its divided data among nearest nodes.

2.5 RDAS: Reputation-based Resilient Data Aggregation System

Carlos R. Perez-Toro, Rajesh K et. al. [5], proposedReputation-based Resilient Data Aggregation System (RDAS), a strong data aggregation protocol that use a reputation-based advance to recognize and cut off cruel nodes in a sensor network andthat develops a distributed known system and relevant it for secure data aggregation in the form of unreliable and spiteful nodes. RDAS is based on a hierarchical cluster form of nodes, were a cluster head clarify data from the cluster nodes to find out the location of an item. The repetition of multiple nodes sense an event to decide what data ought to have been reported by each node. RDAS is able to execute accurate data aggregation in the presence of independently hateful and collude nodes.

2.6 DD: Directed Diffusion

S. Roy, M. Conti, S. Setiaet. al. [6], recently, the research community has proposed a robust data aggregation framework called Directed Diffusion (DD), which combines data from multiple routing schemers.It's a data-centric and application aware paradigm, within the sense that everyone information generated by sensor nodes is called by attribute-value pairs. Such a scheme combines the information coming back from totally different sources en-route to the sink by eliminating redundancy and minimizing the amount of transmissions. During this means, it saves the energy consumption and will increase the network lifespan of WSNs. DD is a climbed and robust communication paradigm for sensor network. DD has some novel features: data centric dissemination, reinforcement-based adaption and in-network data aggregation and caching. DD is highly energy-efficient and robust dissemination in dynamic sensor networks. DD consists of several elements. Data are named using attribute-value pairs. Here, they make the directed diffusion secure against attacks in which compromised nodes contribute false sub aggregate values and analyze the security capabilities and performance of the network. DD is a sensing task, disseminated throughout the sensor network as an internet for named data. This dissemination sets up gradients within the network planned to draw events.

Table 1 shows, the comparison between different data aggregation techniques are as follow with their advantages and disadvantages.

Table 1: Comparison between Different Data Aggregation Technique

Techniques	**Description**	**Advantages**	**Disadvantages**
SIA[7]	It provides opposition against a particular type of attack called stealthy attack where the attacker's goal is to make the user accept deceive aggregation effect	1. data integrity 2. data freshness	Security issue
SDA[8]	dropping, modifying or forging messages, transmitting false aggregate value	It generates secrete key	Security issue
SRDA[3]	It sends the differential data i.e. difference between the sensed data and the reference value instead of the raw sensed data	High security level	Low memory overhead
CDPA[4]	The idea is to use clustering protocol and the polynomial algebraic properties to the protection ofprivacy in the data aggregation sensor nodes form clusters randomly and collectively compute the aggregate result within each cluster.	1.Achieve accurate of polymerization	computation and communication overhead is large
SMART [4]	The main idea is to cut technology and can be added on top of the associated attributes, each node by raw sensory data cut into slice data to hide the original perception data. Its implementation process is divided into three steps: slicing, Mixing, polymerization.	1.Computational overhead is less 2.Better privacy protection	1.The communication overhead is relatively large 2.Data integrity
RDAS[5]	Develops a distributed credit system and applies it for secure data aggregation in the face of unreliable and malicious nodes	1. Handle both colluding and non-colluding faulty nodes 2. provide security	Network Lifetime
DD[6]	It is an information aggregation paradigms for WSNs.	Increase the network lifespan	Small and cheap nodes, less accessible

3. CONCLUSION

Here, we have studied the different data aggregation technique for communication in sensor networks, i.e. data collection from various sensor nodes, data information, and data diffusion and to apprehend how to give information in sensor networks is different from other WSN.Here, various security issues such as data confidentiality, data integrity, authentication and energy efficiency of secure data aggregations are discussed.Cluster based network algorithm is mostly used for low energy consumption and increase the lifetime of network. WSN is an energy constrained network so, the energy is consumed for sending and receiving data, thus, the process ofdata aggregation becomes an important issue and so, optimization is needed.

4. REFERENCES

[1] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputationbased framework for high integrity sensor networks," ACM Trans. Sen. Netw., vol. 4, no. 3, pp. 15:1–15:37, Jun. 2008.

[2] H.-L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, "Energy efficient and fault tolerant multicore wireless sensor network: E2MWSN," in Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, 2011, pp. 1–4.

[3] X.-Y. Xiao, W.-C.Peng, C.-C.Hung, and W.-C. Lee, “Using SensorRanks for in-network detection of faulty readings in wireless sensor networks,” in Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access, ser. MobiDE ‟07, 2007, pp. 1–8.

[4] He, W., Liu, X., Nguyen, H. V., Nahrstedt, K., and Abdelzaher, T. 2011. “Privacy preserving data aggregation for information collection "ACM Transaction Sensor Network. Article 6 (August 2011.DOI = 10.1145/1993042.199)3048.

[5] H.-S. Lim, Y.-S. Moon, and E. Bertino, “Provenancebased trustworthiness assessment in sensor networks,” in Proceedings of the Seventh International Workshop on Data Management for Sensor Networks, ser. DMSN ‟10, 2010, pp. 2–7.

[6] S. Roy, M. Conti, S. Setia, and S. Jajodia, “Secure data aggregation in wireless sensor networks,” Information Forensics and Security, IEEE Transactions on, vol. 7, no. 3, pp. 1040–1052, 2012.

[7] B. Przydatek, D. Song, and A. Perrig, “SIA: Secure Information Aggregation in Sensor Networks”, in proceedings of the 1st International Conference on Embedded Networked Sensor Systems, 2003, pp. 255-265.

[8] L. Hu, D. Evans, “Secure Aggregation for Wireless Networks”, in Symposium on Applications and the Internet Workshops, 27-31 January 2003, pp. 384-391.

[9] H. OzgurSanli, S. Ozdemir, and H. Cam, “SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks”, in IEEE 60th Conference on Vehicular Technology, VTC2004-Fall, Volume 7, 26-29 September 2004, pp. 4650–4654.

[10] S. Ozdemir, “Secure and Reliable Data Aggregatiob for Wireless Sensor Networks”, in proceedings of 4th International Symposium, UCS 2007, Tokya, Japan, 25-28 November 2007, pp. 102-109.

[11] Chan, H., Perrig, A. & Song, D. (2006), secure hierarchical in-network aggregation in sensor networks,in A. Jules, R. N. Wright & S. D. C. di Vimercati,eds, ‘ACM Conference on Computer and CommunicationsSecurity’, ACM, pp. 278–287.